instructions, and what is considered to be the other set of instructions. Nor it is apparent what the Office Action considers to be the first manipulating means, or the other manipulating means that is derived from the first manipulating means. If the rejection is not withdrawn, the Examiner is requested to explain which elements disclosed in the Kocher patent are considered to correspond to each of the claimed first set of instructions, other set of instructions, first manipulating means, and other manipulating means. Without such an explanation, it is respectfully submitted that the Office Action does not set forth a sufficient basis to find a prima facie case of obviousness.

The Office Action acknowledges that the Kocher patent does not disclose the complementation of at least one of the input data and the output data, to provide unpredictability. To this end, therefore, it relies upon the Chow patent. This patent discloses a technique for making a computer program resistant to tampering and reverse engineering. In relevant part, it discloses that the Bit-Exploded and Bit-Tabulated coding techniques described therein can be employed to hide data encryption standard (DES) keys. See, for example, column 20, lines 28-29. Beginning at column 20, line 54, the patent discloses a technique in which the entire DES routine is encoded, and then optimized. As set forth at column 21, lines 9-11, "A completely different set of S-boxes has now been produced which bears no discoverable relation to the original ones and correspond only to the encoded data." Thus, the Chow patent discloses *replacing* the original S-boxes of the DES algorithm with a new set of encoded boxes.

Even if this teaching were to be applied to the system of the Kocher patent, the result would not be the same as the subject matter recited in claim 1. Specifically, there is no suggestion to execute one set of instructions using a first manipulating means, e.g. S-boxes, and to execute another set of instructions using a different set of manipulating means that are derived from the first manipulating means. Rather, since the Chow patent teaches the replacement of the original S-boxes with the encoded S-boxes, all of the instructions would be executed with only the encoded set of S-boxes. There is no suggestion to execute *some*

instructions with the original S-boxes, and *other* instructions with the encoded S-boxes. As can be seen from the above-quoted statement from the Chow patent, the original S-boxes no longer exist in the encoded routine.

For at least these reasons, therefore, it is respectfully submitted that the Kocher and Chow patents do not suggest the subject matter of claim 1, or any of its dependent claims, to a person of ordinary skill in the art, even when these references are considered in conjunction with one another.

Claim 13 recites an electronic component that provides countermeasures against attacks. This component has, among other elements, a processor that executes instructions in a cryptographic algorithm, in accordance with a selected one of plurality of different manipulating means stored in a program memory. The claim further recites "a means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm..." The Office Action acknowledges that the Kocker patent does not discloses this quoted feature, and again relies upon the Chow patent. In doing so, it refers to the same portions of the Chow patent that were cited in the rejection of claim 1. As discussed above, these portions of the patent disclose how the bit encoding technique can be applied to the DES algorithm as whole. They do not, however, disclose the generation of a random value for selecting which of a plurality of different manipulating means is to be employed during a given execution of the algorithm. Nor does not Office Action explain how the reference might be interpreted to suggest this subject matter.

As explained previously, a logical application of the teaching of the Chow patent to the process of the Kocher patent would be to employ an encrypted version of the DES routine in place of the original version. In such an implementation, the same S-boxes are employed for each execution of the routine. There is no disclosure in either reference, or in their combination, to utilize a random value to select from among a plurality of different manipulating means for each execution of the algorithm.

Accordingly, it is respectfully submitted that the Kocher and Chow patents, even when considered in combination, do not suggest the subject matter of claim 13, or its dependent claims.

In view of the foregoing, it is respectfully submitted that all pending claims are patentable over the Kocher and Chow references. If the rejection is not withdrawn, the Examiner is respectfully requested to explain, which particularity, each element in the references that is being interpreted as corresponding to the claim elements identified in the foregoing remarks.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date: June 21, 2006

By: 

James A. LaBarre
Registration No. 28632

P.O. Box 1404
Alexandria, VA 22313-1404
703.836.6620